REMARKS

Claims 1 and 6-21 are rejected under 35 USC 103(a) as being unpatentable over Safai et al. (US 6,167,469), and further in view of Silverbrook (US 6,788,336). Based on the following remarks, the Examiner is asked to reconsider the rejection of claims 1-21. In addition, new claims 22-25 are being added by this amendment.

In the rejection, Safai et al. is characterized as disclosing a processor located within a digital camera for generating a private key and a public key. From an inspection of the patent disclosure, it would appear that the only indication that a key is generated within the camera is a reference in claim 29 to a step of "generating", which comprises "computing and storing a unique private key value...", and in identical language in the "Summary of the Invention" (col. 4, line 11). In both cases, the generating step occurs in a method claim for a camera. However, the detailed description (see, for example, the description of "Image Authentication" in col. 15, line 60 to col. 16, line 50) is completely silent as to any generation of a key in the camera, saying only that the "private key is stored in the camera" (col. 16, line 29) or "embedded in firmware in the camera" (col. 16, line 32). Consequently, the skilled person would receive no enabling guidance from this patent as to what might be tried in order to implement the step of "computing ... a unique private key value..." as part of a method implemented in the camera.

The Examiner acknowledges that Safai et al. says nothing about generating a random seed and using the random seed to generate a private key and a public key. Therefore, Silverbrook is characterized in the rejection as disclosing a processor located within a digital camera that generates a random seed (citing col. 189, lines 45-55 for random number seed R) and teaches using a random seed R to generate keys (citing col. 152, lines 12-13). The applicants respectfully disagree with these observations, in particular finding no such teaching or suggestion in Silverbrook that a processor located within a digital camera generates a random seed.

As the Examiner noted, Silverbrook in column 151 says that "random number generators are also often used to generate keys" but then Silverbrook goes on to say (lines 12-13) that "it is therefore best to say at the moment, that all generators are insecure for this purpose". With regard to such a concern for security, Silverbrook says in col. 173, lines 51-52 that "the seed for R must NOT be generated with a computer-run random number generator" (emphasis in original wording in the patent). Likewise, K1 and K2 (the public and private keys) "must NOT be generated with a computer-run random number generator" (col. 189, lines 13-14 and 35-36). Instead, according to Silverbrook, these numbers are physically generated random numbers gathered from a physically random phenomenon, that is, actually generated in a way that is not deterministic, e.g., "to set K1 (or K2), a person can toss a fair coin 160 times, recording heads as 1, and tails as 0" (col. 189, lines 16-19 and 38-39).

Therefore, in Silverbrook, the authentication chips used in his camera/printer device, which store the keys and the random number, are programmed with these non-deterministic results – the random seed R and the keys K1 and K2 – in a secure environment,

> Authentication Chips must be programmed with logically secure information in a physically secure environment. Consequently the programming procedures cover both logical and physical security. Logical security is the process of ensuring that K1, K2, R, and the M[n] values are generated by a physically random process, and not by a computer……Physical security is the process of ensuring that the programming station is physically secure, so that K1 and K2 remain secret, both during the key generation stage and during the lifetime of the storage of the keys. (col. 200, lines 39-41)

It is clear from the preceding citations that Silverbrook teaches unequivocally that an in-camera processor should NOT be used to generate a random seed, and an in-camera processor should NOT be used to generate any keys. These citations are also helpful in understanding the section of Silverbrook (col. 189) that the Examiner cited, where Silverbrook says that "R must be changed only by the

Authentication Chip, and not set to any chosen value by a caller" (lines 48-50). It should be clear from the preceding paragraphs that R is not generated by the Authentication Chip, but that the value of R is only set into the Chip by programming a value of R (predetermined from a physically random phenomenon) in a secure environment. Thus, the reference to "changing" R could reasonably mean that the Chip is re-programmed in the secure environment, or that a new Chip is substituted for the old Chip.

The Examiner argues that claims 1 and 6-21 are obvious over Safai et al. in view of Silverbrook. These claims include a common limitation, represented in paragraph (a) of claim 1 as "a processor located within the digital camera for generating a random seed and for using the random seed to generate a private key and a public key" (paragraph(a)). The Examiner argues that it would be obvious to incorporate the teachings of Silverbrook regarding (a) *a digital camera generating a random seed* and (b) *using the random seed to generate keys in the digital camera* disclosed by Safai et al. However, it is clear from the preceding citations that Silverbrook teaches unequivocally that an in-camera computer or processor should NOT be used to generate a random seed, and the in-camera computer or processor should NOT be used to generate any keys. The Examiner further concludes that the motivation for combining Safai et al, and Silverbrook "would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing". However, this would appear to be in direct opposition to the teaching of Silverbrook. Indeed, Silverbrook is arguing that generation of the keys by a computer or processor in the camera, or by any other form of computer-run random number generation, in fact would greatly compromise security.

It is respectfully suggested that a rejection under 35USC103(a) may not be maintained unless, among other requirements, (1) all of the claim limitations are taught or suggested by the prior art, and (2) there is some suggestion or motivation in the first place to draw upon the cited prior art, such that each claim limitation is taught or suggested in the prior art. These are among the requirements for a *prima facie* case of obviousness. MPEP 2143.01 –

2143.03. Neither Safai et al. nor Silverbrook, either alone or in combination, teach or suggest providing a processor located within the digital camera for generating a random seed, and neither Safai et al. nor Silverbrook, either alone or in combination, show any suggestion or motivation for using a random seed in a processor located within the digital camera to generate a private key and a public key. Accordingly, the rejection of pending claims 1 and 6-21 does not meet the aforementioned requirements, either wholly or in part, and is accordingly traversed.

In rejecting claims under 35 U.S.C. §103(a), the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).* Only if that burden is met does the burden of coming forward with evidence or argument shift to the applicant. *Id.* " A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993)* quoting *In re Rinehart, 189 USPQ 143, 147 (CCPA 1976).* If the Examiner fails to establish a *prima facie* case, the rejection is improper and will be overturned. *In re Fine, 5USPQ2d 1596, 1598 (Fed. Cir. 1988).* For reasons as set forth above, the Examiner has not established a *prima facie* case, and the claims 1 and 6-21 therefore should be in allowable condition as they stand.

With regard to dependent claims 16-21, where each claim states that the algorithm (producing the private key) is deleted from the firmware memory after the private key is generated, the Examiner alleges that Safai et al. discloses that the private key is produced using an algorithm stored in the firmware memory. As stated in the preceding paragraphs, there appears to be nothing in Safai et al. explicitly indicating such an algorithm or where it might be stored. Then, the Examiner alleges that Silverbrook provides motivation for deleting such an algorithm in the camera in order to deter an attack after the key has been generated. However, as stated in the preceding paragraphs, Silverbrook unequivocally teaches that such an algorithm should never be in the camera in the first place. Thus its disclosure would not provide the suggested motivation, since

Silverbrook unequivocally motivates a skilled person away from applicants' invention, that is, away from storing such an algorithm in the camera at any time or point. Accordingly, claims 16-21 are believed to be independently patentable over the combination of the teaching of Safai et al. and Silverbrook.

Claims 2-5 are rejected under 35 USC 103(a) as being unpatentable over Safai and Silverbrook as applied to claim 1 above, and further in view of Glass et al. (US 6,332,193). Claims 2-5 are dependent on claim 1, and therefore include all the features thereof. Accordingly, for the reasons set forth above with regard to claim 1, claim 2-5 are also believed to be patentable. However, notwithstanding the allowability of claims 2-5 for reasons as stated above, Glass et al. does not disclose or suggest anything relating to use of the random noise level in the captured image to produce a random seed – as this is particularly claimed in claims 2 and 3. Furthermore, Glass et al. does not disclose or suggest anything relating to one or more algorithms for producing a random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing – as this is particularly claimed in claims 4 and 5. Accordingly, claims 2-5 are believed to be independently patentable over the combination of the teaching of Safai et al., Silverbrook and Glass et al.

New claims 22-25 are being added by this amendment to cover a further definition of the invention. More specifically, addressing the new claims in part, claim 22 relates to "a processor located within the digital camera for generating the private key, at least in part, from a physically random process", (see, for support, processing random image data (page 9, lines 26-28) rather than output from a pseudo-random number generation algorithm (page 9, lines 23-25). Claim 23 further defines the physically random process to be dependent upon a random seed produced from a random noise level in a captured image (lines 26-28), where (claim 24) "the random noise level is produced by random dark field image data taken from the sensor" (line 28). Claim 25 identifies variable-gain circuitry similar to that of claim 3. As indicated above, new matter is not being added.

If there are any formal matters remaining after this response, Applicants' attorney would appreciate a telephone call to attend to these matters.

In view of the foregoing, this application is believe to be in condition for allowance, the notice of which is respectfully requested.

The Commissioner is hereby authorized to charge any fees in connection with this communication to Eastman Kodak Company Deposit Account No. 05-0225. ***A duplicate copy of this communication is enclosed.***

Respectfully submitted,

Pamela R. Crocker

Pamela R. Crocker
Attorney for Applicant(s)
Registration No. 42,447

PRC:cjm
Telephone: (585) 477-0553
Facsimile: (585) 477-4646